Homeland Security

Daily Open Source Infrastructure Report 17 November 2015

Top Stories

- A Pacific Gas and Electric Co. pipeline was shut down after it ruptured and exploded November 13 in Kerns County, California, killing 1 person and injuring 2 others. – *Associated Press* (See item **2**)

- Kia Motors issued a recall November 6 for 256,000 of its Soul vehicles model year 2014 – 2016 due to a manufacturing error in the pinion plug that could loosen and fall out, causing a dangerous inability to control the vehicle. – *New York Times* (See item **3**)

- A City Sightseeing tour bus veered out of control and ran down several people before crashing into a construction site in San Francisco's Union Square November 13, leaving at least 20 people injured. – *Fox News; Associated Press* (See item **10**)

- A Maryland couple was convicted November 12 in connection to orchestrating a scheme to defraud Washington, D.C. Medicaid out of more than $80 million through one of the defendant's company, Global Health Care Services of the District. – *Washington Post* (See item **19**)

Fast Jump Menu

Energy Sector

1. *November 15, Associated Press* – (California) **More repairs ordered for pipe after California oil spill.** The Pipeline and Hazardous Materials Safety Administration ordered Plains All American Pipeline November 13 to purge a neighboring oil pipeline and make repairs following a May 19 rupture and spill of more than 100,000 gallons of crude on the California coast from another company-owned pipeline that remains idled.
Source: http://fuelfix.com/blog/2015/11/15/more-repairs-ordered-for-pipe-after-california-oil-spill/

2. *November 14, Associated Press* – (California) **1 killed, 2 injured after gas line explodes in California.** A Pacific Gas and Electric Co. pipeline was shut down after it ruptured and exploded November 13 in Kerns County, California, killing 1 person and injuring 2 others. The line was cut by someone using heavy equipment and fire crews were able to put out the fire that also destroyed a nearby home.
Source: http://www.foxnews.com/us/2015/11/14/1-killed-2-injured-after-gas-line-explodes-in-california/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

3. *November 13, New York Times* – (National) **Kia issues a second recall of Soul models in 2 years.** Kia Motors issued a recall November 6 for 256,000 of its Soul vehicles model year 2014 – 2016 due to a manufacturing error in the pinion plug, a part of the steering assembly that could loosen and fall out, causing a dangerous inability to control the vehicle. The recall follows an earlier recall of 52,000 Kia Soul vehicles for the same issue.
Source: http://www.nytimes.com/2015/11/14/business/kia-issues-a-second-recall-of-soul-models-in-2-years.html

4. *November 13, U.S. Department of Labor* – (New York) **Employee struck by forklift at Schenectady recycling facility.** The Occupational Safety and Health Administration cited Tomra NY Recycling LLC for 1 willful violation for defective forklifts and 2 serious violations for other hazards November 13 following an incident in which an employee was struck by a forklift at its Schenectady, New York facility. Proposed fines total $84,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29040

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *November 15, Chicago Sun-Times* – (Illinois) **Wheaton financial firm owner charged with wire fraud.** The owner of Illinois Stock Transfer Company in Wheaton was charged November 12 for 10 counts of wire fraud after stealing more than $1.2 million from a client's fund account and using the funds for his company's corporate taxes, payroll, and business expenses from 2012 to 2014.
Source: http://chicago.suntimes.com/news/7/71/1103407/wheaton-financial-firm-owner-charged-wire-fraud

6. *November 14, Softpedia* – (National) **PoS malware spread via weaponized Microsoft Word documents.** Researchers from Proofpoint discovered the point-of-sale (PoS) malware dubbed AbaddonPOS was a part of a malware-delivery campaign allowing attackers to download other malware from Command and Control servers (C&C) using its own custom protocol via Microsoft Word documents and malicious Web sites, in an attempt to steal credit and debit card transaction data.
Source: http://news.softpedia.com/news/pos-malware-spread-via-weaponized-microsoft-word-documents-496155.shtml

Transportation Systems Sector

7. *November 15, WKRG 5 Mobile* – (Alabama) **ID released on fatal Chunchula wreck.** Highway 45 in Chunchula, Alabama, was shut down for approximately 3 hours November 14 while officials cleared debris from a fatal 2-vehicle crash killed 1 person and left 4 others injured.
Source: http://wkrg.com/2015/11/14/fatal-wreck-on-highway-45-in-chinchilla/

8. *November 15, WKBW 7 Buffalo* – (New York) **Man killed after wrong way crash overnight on I-190.** Northbound lanes of Interstate 190 in Buffalo were shut down for approximately 5 hours November 14 after a fatal 3-vehicle crash left 1 person dead and a second person injured.
Source: http://www.wkbw.com/news/man-killed-after-wrong-way-crash-overnight-on-i-190

9. *November 14, WPIX 11 New York City* – (New York) **Major delays at all metro area airports due to equipment failure.** The Federal Aviation Administration reported that flights at all New York and metro area airports were delayed up to 13 hours November 14 due to equipment failure.
Source: http://pix11.com/2015/11/14/major-delays-at-all-metro-area-airports-due-to-equipment-failure

10. *November 14, Fox News; Associated Press* – (California) **At least 20 injured, 6 critically when out-of-control tour bus crashes in San Francisco.** A City

Sightseeing tour bus veered out of control and ran down several people before crashing into scaffolding lining a construction site in San Francisco's Union Square November 13, leaving at least 20 people injured. Authorities are investigating the cause of the accident.
Source: http://www.foxnews.com/us/2015/11/14/several-hurt-as-careening-tour-bus-crashes-in-san-francisco/

11. *November 13, Brattleboro Reformer* – (Vermont) **Frozen pea spill causes shut down on Route 9.** Route 9 between MacArthur Road and Hamilton Road in Marlboro was shut down for several hours November 13 after a semi-truck overturned spilling 42,000 pounds of frozen peas. An initial investigation found that the driver was operating the vehicle with seven violations, prompting both the driver and the truck to be taken out of service.
Source: http://www.reformer.com/localnews/ci_29113807/brattleboro-reformer

12. *November 13, KOLN 10 Lincoln/KGIN 11Grand Island* – (Nebraska) **18-year-old senior from Syracuse High killed in crash near Bennet.** Westbound lanes of Highway 2 in Lancaster County were closed for 6 hours November 12 following a fatal accident involving a vehicle that crashed into a grain truck and caught fire, killing 1 person and injuring another.
Source: http://www.nbcneb.com/home/headlines/One-Confirmed-Dead-Following-Accident-Near-176th-and-Hwy-2-347315792.html

Food and Agriculture Sector

13. *November 15, Hancock County Ellsworth American* – (Maine) **Fire delays opening of newly built Trenton seafood processing plant.** Trenton officials reported November 15 that over 9 fire departments remained onsite for nearly 5 hours at the Bar Harbor owned-Acadia Aqua Farms, a mussel processing facility after a November 14 fire caused extensive damage to the facility. No injuries were reported.
Source: http://www.ellsworthamerican.com/featured/area-crews-fight-trenton-blaze-saturday-night

14. *November 13, U.S. Food and Drug Administration* – (National) **Virginia Diner, Inc. issues allergy alert on undeclared peanut allergen in Pecan Turtledoves Chocolate Caramel Pecan Clusters (Candy).** Wakefield, Virginia-based Virginia Diner, Inc. issued a voluntary nationwide recall of 10-ounce cans of Pecan Turtledoves Chocolate Caramel Pecan Clusters November 13 due to undeclared peanut allergens after a customer discovered Peanut Turtledoves instead of Pecan Turtledoves. Products were distributed and sold through fundraising organizations.
Source: http://www.fda.gov/Safety/Recalls/ucm472743.htm

15. *November 13, U.S. Food and Drug Administration* – (National) **FDA releases groundbreaking food safety rules for produce farms and imported food to modernize and strengthen food safety system.** The U.S. Food and Drug Administration (FDA) announced November 13 that it was finalizing provisions outlined in the 2011 FDA Food Safety Modernization Act to establish verifiable safety

standards for produce farms and hold importers accountable for the safety of their products by formalizing industry accountability and best practices.
Source:
http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm472426.htm

16. *November 13, U.S. Food and Drug Administration* – (National) **Giant Eagle voluntarily recalls Apricot Logs and Poppyseed Logs due to an undeclared milk allergen.** Giant Eagle and Market District supermarkets in several states issued a recall of 460 Apricot and Poppyseed Logs November 12 after a quality review discovered that the products had undeclared milk allergens.
Source: http://www.fda.gov/Safety/Recalls/ucm472555.htm

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

17. *November 14, WLWT 5 Cincinnati* – (Ohio) **UC Health patient information compromised after email error.** The University of Cincinnati Academic Health Center in Ohio will notify 1,000 patients that their personal information may have been compromised on 9 occasions dating back to August 2014 after emails containing protected health information were mistakenly sent to an incorrect email address. Hospital officials blocked further emails from going to the unauthorized domain and continue to investigate the incident.
Source: http://www.wlwt.com/news/uc-health-patient-information-compromised-after-email-error/36450504

18. *November 13, KWQC 6 Davenport* – (Iowa) **Illinois data breach; agency posts personal information on public website.** The Illinois Department of Insurance will notify an unknown amount of individuals after the department inadvertently sent filings from Blue Cross Blue Shield to the System for Electronic Rate and Form Filing (SERFF) database, which posted the information on its publicly available Web site. The department is taking steps to prevent future disclosures after receiving a complaint that Social Security numbers from Blue Cross Blue Shield could be seen.
Source: http://kwqc.com/2015/11/13/illinois-data-breach-agency-posts-personal-information-on-public-website/

19. *November 12, Washington Post* – (Washington, D.C.) **Federal jury convicts Md. couple in $80 million D.C. Medicaid fraud case.** A Maryland couple was convicted November 12 in connection to orchestrating a scheme to defraud Washington, D.C. Medicaid out of more than $80 million between 2009 and 2014 through one of the defendant's company, Global Health Care Services of the District. The pair enlisted relatives and others to sign up and coach Medicaid recipients who received kickbacks for submitting false claims for health care that was never provided.
Source: https://www.washingtonpost.com/local/public-safety/federal-jury-convicts-md-couple-in-80-million-dc-medicaid-fraud-case/2015/11/12/927dfa10-8988-11e5-be8b-

1ae2e4f50f76_story.html

Government Facilities Sector

20. *November 15, Boston Herald* – (Massachusetts) **FBI: Weapons missing from Worcester Army Reserve building.** The FBI reported November 15 that it is working with State and local law enforcement in an investigation after an unknown amount of weapons were taken in a burglary at the Lincoln W. Stoddard U.S. Army Reserve Center in Worcester November 14.
Source: http://www.bostonherald.com/news/local_coverage/herald_bulldog/2015/11/fbi_weapons_missing_from_worcester_army_reserve_building

21. *November 14, Petersburg Progress-Index* – (Virginia) **1 man arrested, charged for courthouse bomb threat.** Police arrested a suspect November 14 for allegedly phoning in a bomb threat that closed the Hopewell Courts Facility and surrounding businesses in Virginia November 13.
Source: http://www.progress-index.com/article/20151114/NEWS/151119857

22. *November 13, Tulsa World* – (Oklahoma) **'One of the worst I've seen': Oklahoma wildfires destroy homes, scorch 45,000-plus acres.** Crews worked November 12 to contain a wildfire that burned 45,680 acres and destroyed several structures and outbuildings in Nowata, Washington, and eastern Osage counties in Oklahoma.
Source: http://www.tulsaworld.com/news/local/one-of-the-worst-i-ve-seen-oklahoma-wildfires-destroy/article_d27699ff-937a-5281-9d60-95864e940e6d.html

23. *November 13, U.S. Attorney's Office, Northern District of Texas* – (Texas) **Federal jury convicts brothers in visa fraud case.** Two brothers were convicted November 13 for orchestrating a scheme to commit H-1B visa fraud to secure a low-cost workforce at their company, Dibon Solutions in Carrollton, Texas, from March 2005 to February 2011. The pair sponsored workers through the program with the stated purpose of working for their information technology consulting company, but instead charged other third-party companies to hire the workers while the brothers received payments from the companies in return.
Source: http://www.justice.gov/usao-ndtx/pr/federal-jury-convicts-brothers-visa-fraud-case

24. *November 12, Nextgov* – (National) **OPM's $20 million contract for post-hack ID protection violated federal contracting rules.** The inspector general of the U.S. Office of Personnel Management announced November 12 that a $20 million contract to offer identity theft protection to some 4.2 million Federal employees who had their personal information hacked violated the Federal Acquisition Regulations and the agency's own policies after it was awarded. Investigators found significant deficiencies in the contract award process.
Source: http://www.nextgov.com/cybersecurity/2015/11/opms-20-million-contract-post-hack-id-protection-violated-federal-contracting-rules/123649/

For another story, see item **18**

Emergency Services Sector

25. *November 15, Softpedia* – (National) **Police body cameras shipped with pre-installed Conficker virus.** iPower Technologies found that body cameras sold to police forces around the U.S. were pre-infected with the Conficker worm (Win32/Conficker.B!inf.), which was discovered in the device's internal drive and records data that can be downloaded onto a computer via Universal Serial Bus (USB) cable. Researchers attempted to notify Martel Electronics, the company that sells the body cameras.
Source: http://news.softpedia.com/news/police-body-cameras-shipped-with-pre-installed-conficker-virus-496177.shtml

26. *November 15, KTRK 13 Houston* – (Texas) **3 escape juvenile detention center in downtown Houston, guard beaten.** Police are searching for three juvenile inmates who escaped from the Harris County's Juvenile Justice Center in Houston by overpowering and beating a guard November 15.
Source: http://abc13.com/news/three-teens----including-a-murder-suspect----escape-detention-center/1085707/

27. *November 13, North Country Gazette* – (New York) **Investigating 911 outage to 400,000 in lower Hudson Valley.** The New York State Department of Public Service announced November 13 that it is investigating a 4 hour 9-1-1 outage that potentially impacted over 400,000 Verizon New York and Frontier Communications customers in Westchester, Putnam, Ulster, and Sullivan counties.
Source: http://www.northcountrygazette.org/2015/11/13/911_outage-2/

Information Technology Sector

28. *November 16, Securityweek* – (International) **Thousands of sites infected with Linux encryption ransomware.** Researchers from Dr. Web reported that approximately 2,000 Web sites were compromised by the Linux file-encrypting ransomware dubbed Linux.Encoder1, that targets the root and home files, web servers, backups, and source code via a downloaded file containing the public RSA key used to store AES keys that adds .encrypt extension to each file, allowing files to be nearly impossible to recover without paying a ransom to the attackers. A patch was released, but experts warned that attackers may update the malware to make file decryption more difficult.
Source: http://www.securityweek.com/thousands-sites-infected-linux-encryption-ransomware

29. *November 16, IDG News Service* – (International) **State-sponsored cyberspies inject victim profiling and tracking scripts in strategic websites.** Security researchers from FireEye discovered an attack campaign dubbed WITCHCOVEN, which has injected computers profiling and tracking scripts into over 100 Web sites involved in international business travel, diplomacy, energy production and policy, international economics, and official government work. The malware was designed to identify users of interest and target such users with exploits designed for their specific computer and

software configurations.
Source: http://www.computerworld.com/article/3005270/malware-vulnerabilities/state-sponsored-cyberspies-inject-victim-profiling-and-tracking-scripts-in-strategic-websites.html#tk.rss_security

30. *November 16, InfoWorld* – (International) **Microsoft fixes Hyper-V bug in Windows.** Microsoft released patches for vulnerabilities in its Hyper-V hypervisor software affecting several Windows Servers, including a flaw in the central processing unit (CPU) chip set that issues instructions and causes the host system into a nonresponsive state, resulting in a denial-of-service condition for users' operating systems. No attacks in the wild have been reported.
Source: http://www.infoworld.com/article/3005238/security/microsoft-fixes-hyper-v-bug-in-windows.html

31. *November 16, Softpedia* – (International) **A quarter of web-accessible devices have vulnerable firmware.** Researchers from EURECOM and Ruhr University in Bochum, Germany, released a study confirming the weak state of security for Internet of Things (IoT) devices included cross-site scripting (XSS) vulnerabilities, cross-site request forgery (CSRF) vulnerabilities, SQL injection (SQLi) vulnerabilities, and remote code/command execution (RCE) vulnerabilities which can grant attackers access to devices, spy on users, steal data, and rewrite the firmware to perform other malicious activities.
Source: http://news.softpedia.com/news/a-quarter-of-web-accessible-devices-have-vulnerable-firmware-496229.shtml

32. *November 16, Securityweek* – (International) **Libpng Library updated to patch vulnerabilities.** The official Portable Network Graphics (PNG) reference library, Libpng released an update addressing several memory corruption vulnerabilities in all its versions from 1.6.18 – 1.0.63, affected by a potential out-of-bounds read in the png_set_tIME() and png_convert_to_rfc1123() functions, and an out-of-bounds write issue in the png_get_PLTE() and png_set_PLTE() functions that failed to check for an out-of-range palette when reading or writing PNG files. The flaws were patched with the release of updated versions.
Source: http://www.securityweek.com/libpng-library-updated-patch-vulnerabilities

33. *November 15, Softpedia* – (International) **Compromised Web site fools security vendor, continues to infect users.** Researchers from Palo Alto Networks reported that the CryptoWall 3.0 ransomware, that previously affected all users via the Angler Exploit Kit when users visited the Web site, cxda.[.]gov[.]cn, was still active and compromised 4,000 additional Web sites despite initial reports that revealed the malicious campaign had stopped. Researchers revealed a "dormant" and "filtering" functionality imbedded in the campaign's malicious code allowed attackers to go unnoticed depending on the Web sites' source Internet Protocol (IP) and user agent.
Source: http://news.softpedia.com/news/compromised-website-fools-security-vendor-continues-to-infect-users-496178.shtml

34. *November 13, Softpedia* – (International) **Oil and gas companies indirectly put at risk by vulnerabilities in ERP systems.** Researchers from ERPScan presenting at Black Hat Europe 2015 showed how a vulnerability in an enterprise resource planning (ERP) suite from SAP and Oracle used inside oil and gas companies, could allow an attacker to gain access into operation technology (OT) infrastructure through connected applications that are insecure. The researchers also determined that misconfigurations, the presence of unnecessary privileges, and custom code provided entry or access escalation points for attacks.
Source: http://news.softpedia.com/news/oil-and-gas-companies-indirectly-put-at-risk-by-vulnerabilities-in-erp-systems-496124.shtml

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: http://www.it-isac.org

Communications Sector

Nothing to report

Commercial Facilities Sector

35. *November 15, WBAY 2 Green Bay* – (Wisconsin) **Little Chute residents allowed to return to apartment complex after evacuation.** Wisconsin police reported November 15 that residents at a Little Chute apartment complex were evacuated for nearly 3 hours November 14 after a 73-year-old man armed with a handgun barricaded himself in his apartment. Several police departments responded to the scene and resolved the event without incident.
Source: http://wbay.com/2015/11/15/little-chute-residents-allowed-to-return-apartment-complex-after-evacuation/

36. *November 15, Kendallville News Sun* – (Indiana) **Fire forces evacuation of apartment complex.** An Angola fire official reported November 15 that an accidental fire at Lakeland Apartments November 14 prompted an evacuation of 100 residents and injured 2 others. Fire crews contained the incident.
Source: http://www.kpcnews.com/news/latest/heraldrepublican/article_d0e9c9e7-19aa-59c0-9a07-ffc5fa12fcee.html

37. *November 13, Phoenix Arizona Republic* – (Arizona) **Airborne irritant spurs Phoenix apartments evacuation.** The Phoenix Fire Department reported November 13 that about 30 residents were evacuated from an apartment complex after 5 residents reported having troubled breathing from an unidentified airborne substance that caused eye, nose, and throat irritation. The injured residents were treated at the scene and the cause of the incident is under investigation.
Source:

http://www.azcentral.com/story/news/local/phoenix/breaking/2015/11/14/airborne-irritant-spurs-phoenix-apartments-evacuation/75758294/

38. *November 13, U.S. Department of Labor* – (Texas) **Furniture manufacturer, staffing agency expose workers to hazards twice in 14 months.** The Occupational Safety and Health Administration cited MooreCo Inc., November 12 for 3 repeated and 6 serious violations and placed the company in its Severe Violator Enforcement Program, and cited ManPower Group US Inc., for 1 repeated violation for exposing workers to moving machine parts and failing to shut down machinery properly following two incidences in which temporary workers were seriously injured when inadequately guarded machines pulled in both employees, causing finger amputations and skin removal. Fines total $122,500 for MooreCo Inc., and $38,500 for Manpower Group US Inc.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29043

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.